

WellDatabase

Privacy Policy

Version 2026.10 — ctrlDev, LLC d/b/a WellDatabase — Effective 13 August 2026

1. Who we are and what this policy covers

This policy explains what personal information ctrlDev, LLC d/b/a WellDatabase (“WellDatabase”, “we”, “us”) collects, why we collect it, who we share it with and what you can do about it. Our principal place of business is 4 Waterway Square Place, Suite 477, The Woodlands, TX 77380, United States.

It covers our marketing website at welldatabase.com, the WellDatabase application at app.welldatabase.com, our API, and the sales and support activity around them.

What it does not cover. Where we process personal data on a customer’s behalf as part of providing the Services, that customer decides what happens to it and we act on their instructions. That processing is governed by our *Data Processing Agreement* at welldatabase.com/dpa, not by this policy. This policy covers the information for which WellDatabase itself decides the purpose — account and billing records, support and sales correspondence, website and product analytics, and recorded calls.

Contact. privacy@welldatabase.com for anything in this policy. legal@welldatabase.com for formal legal notices.

2. The short version

- We are not an advertising business. We do not sell personal information, we do not share it for cross-context behavioral advertising, and we do not use it to train large language models or other AI models.
- We collect what we need to run accounts, take payment, provide support, keep the platform secure, and understand how the product is used.
- We record product sessions to diagnose performance problems. We say so below, in detail, because it is the least obvious thing we do.
- We record video calls with customers, with notice.
- Everything is hosted in the United States.
- The oil and gas records in the product come from public government filings. They contain names. You cannot search, filter or aggregate the product by a person’s name, and we have no plans to make that possible.

3. What we collect, where it comes from, and why

The categories below are the categories of personally identifiable information we collect, as required by California Business and Professions Code section 22575.

Category	Examples	Where it comes from	Why we have it
Identifiers and contact details	Name, business email address, telephone number, job title, employer, postal address	You, when you register, request a demo, sign an Order or contact us; your colleagues; your employer’s account administrator	To create and administer your account, to provide support, and to correspond with you about the Services
Account and credential data	Username, hashed password, account role and permissions,	You, and our systems	To let you sign in, to enforce seat limits, and to detect

	authentication events		unauthorized access
Billing and transaction data	Billing contact, billing address, invoice and payment history, plan and subscription details	You, and Stripe	To take payment, issue invoices, and meet tax and accounting obligations
Payment instrument data	Card number, expiry, security code	You, entered directly into Stripe	We do not receive or store full card numbers. Stripe processes these as a controller for its own purposes
Commercial and contract data	Order and quote records, signature audit trail, IP address of the signatory	You, and PandaDoc	To prepare, deliver and evidence execution of agreements
Support and sales correspondence	Emails, chat messages, support tickets, notes of calls and meetings	You, and our team	To answer questions, resolve problems and keep a record of what was agreed
Usage and device data	IP address, browser and device type, operating system, pages and features used, in-application events, referring page, timestamps	Automatically, from your browser and our application	To keep the Services secure and available, to diagnose faults, and to understand which features are used
Session recordings	A replay of a session in the application, which may capture what was typed into or displayed in the Services, including search terms and query parameters	Automatically, in the application, via PostHog	To reproduce and diagnose performance problems and errors. See Section 5
Call recordings and transcripts	Video, audio, image, transcript and automated summary of calls with WellDatabase personnel	Fathom, when a call is recorded	To keep an accurate record of customer conversations and to brief colleagues. See Section 5
Marketing data	Business contact details, campaign and email engagement, website visit history	You, our website, and HubSpot	To send business communications about the Services and to measure whether they were useful

We do not collect sensitive personal information as that term is used in US state privacy laws — no government identifiers, precise geolocation, biometric data, health data, racial or ethnic origin, religious beliefs, sexual orientation, or contents of private communications other than the correspondence you send us. We do not knowingly collect information from anyone under 18. See Section 12 (Children).

4. Our legal bases, where the GDPR applies

Where the EU or UK General Data Protection Regulation applies to our processing, we rely on the following legal bases.

Purpose	Legal basis
Creating and administering accounts, providing the Services, taking payment, providing support	Performance of a contract, or steps taken at your request before entering into one — Article 6(1)(b)
Keeping the Services secure, detecting fraud and abuse, diagnosing faults, understanding feature usage, improving the	Our legitimate interests in operating, securing and improving a service our customers rely on, and in offering it to businesses

product, and marketing to business contacts	likely to find it useful — Article 6(1)(f). We have assessed these interests against your rights and keep a record of that assessment
Session recording, call recording, and non-essential cookies	Consent — Article 6(1)(a). You may withdraw consent at any time; withdrawal does not affect processing carried out before you withdrew it
Retaining invoices, tax records and signed agreements	Compliance with a legal obligation — Article 6(1)(c)

Providing your name, business email and billing details is a contractual requirement. If you do not provide them we cannot create an account or provide the Services. Everything else is optional.

No automated decision-making. We do not make decisions producing legal or similarly significant effects about you by automated means, and we do not carry out profiling of that kind.

5. Cookies, analytics and recording

Cookies. We use cookies and similar technologies that are necessary to make the Services work — signing you in, keeping your session, remembering preferences, and protecting against abuse. We also use analytics cookies, which are not necessary. Most browsers accept cookies by default and let you refuse or delete them; some features will not work correctly if you do.

Website and application analytics. We use Google Analytics on both welldatabase.com and app.welldatabase.com to understand traffic and how people move through the product.

Product analytics and session recording. We use PostHog for product analytics and session recording inside the application. A session recording is a reconstruction of what happened on screen during a session.

- Because reproducing a fault requires knowing what was entered, a recording may capture information typed into or displayed in the Services, including search terms and query parameters.
- We use it only to identify usage trends, diagnose errors, and monitor and improve the performance, reliability and usability of the Services.
- We do not use it for marketing or advertising, we do not sell or license it, and we do not make it available to anyone other than the subprocessors listed at welldatabase.com/subprocessors.
- Session recordings are retained for no longer than thirty (30) days and are then deleted.
- Where a recording captures a customer's confidential information, it stays subject to the confidentiality obligations in our Terms and Conditions.
- Form inputs are masked in our session recording configuration, so values typed into a form are obfuscated before a recording is stored.
- Payment details are entered directly into our payment provider's own embedded form. That form is not visible to our session recording and cannot be captured by it.

In-application chat. We use HubSpot for support ticketing and in-application chat. Messages you send through it are retained as support correspondence.

Recorded calls. We use Fathom to record, transcribe and summarize video calls, including calls with customers and prospective customers. Recording is announced at the start of the call and is noted in the meeting invitation. If you do not want to be recorded, tell us and we will turn it off — the call goes ahead either way. Recordings and transcripts are used internally, to keep an accurate record of what was discussed and to brief colleagues. They are not published, sold or used for marketing.

6. Who we share information with

We share personal information with the following categories of third parties, and no others:

- Service providers who process it on our behalf — cloud hosting, email delivery, payment processing, customer relationship management and support, electronic signature, analytics and call recording. Each is bound by a written contract that limits them to processing for our purposes. The current list, with the purpose and data categories for each, is published at welldatabase.com/subprocessors and is kept up to date.
- Professional advisers — our lawyers, accountants and auditors, under a duty of confidentiality.
- Authorities and parties to legal process, where we are required by law, regulation, subpoena or court order, or where we need to establish, exercise or defend legal claims. Where we are legally permitted to tell you first, we will.
- An acquirer, in connection with a merger, acquisition, financing or sale of assets, subject to confidentiality and to this policy continuing to apply until you are given notice of any change.

We give customers at least thirty (30) days' notice before engaging a new subprocessor or replacing an existing one, and customers may object on reasonable data protection grounds.

7. What we do not do

- We do not sell personal information, and we have not sold personal information in the preceding twelve months.
- We do not share personal information for cross-context behavioral advertising, and we have not done so in the preceding twelve months.
- We do not use personal information, and we do not make it available to anyone else to use, to train large language models or other artificial intelligence models.
- We do not use analytics or session recording data for marketing or advertising.
- We do not sell sensitive personal data.
- We do not buy marketing lists containing personal data of individuals in the EEA or the United Kingdom.

8. Do Not Track and Global Privacy Control

Global Privacy Control. We honor the Global Privacy Control signal. Because we do not sell or share personal information, the signal has nothing to opt out of — but where it is present we also treat it as a request not to load non-essential analytics.

Do Not Track. There is still no common industry standard for how a website should respond to a browser Do Not Track signal. We treat Do Not Track the same way we treat Global Privacy Control, as described above. This paragraph is provided under California Business and Professions Code section 22575(b)(5).

Third-party collection across sites. We do not permit third parties to collect personally identifiable information about your online activities over time and across third-party websites when you use our sites. This paragraph is provided under section 22575(b)(6).

9. Names in the oil and gas records

The Content in WellDatabase is compiled from public government records — regulatory filings, permits, production reports and lease records maintained by state agencies and made lawfully available by them. Those records contain names, because the underlying filings do: mineral owners, lessees, operators and their officers.

Two things are worth stating plainly.

- We do not enrich, append to, score or make assertions about any individual. We reproduce what the public record says, and we do not warrant that it is accurate or current.
- The product cannot be searched, filtered, sorted or aggregated by a person's name. Every filter dimension is geological, operational or corporate — well, lease, formation, basin, county, operator, date, volume. This is a deliberate design constraint, not an oversight.

If you believe information about you in a public record we reproduce is inaccurate, the correction has to be made at the source agency, because we take a feed of what they publish. Write to privacy@welldatabase.com and we will tell you which agency and which record.

10. How long we keep information

We keep personal information for as long as we need it for the purpose we collected it for, and then delete it. In practice:

- **Session recordings — thirty (30) days.** This is a fixed period and we do not extend it.
- **Account, profile and content data** — for as long as the account is open, and then through the ninety (90) day post-termination export window described in our Terms and Conditions, after which it is securely deleted.
- **Invoices, payment records, tax records and signed agreements** — for as long as tax, accounting and limitation-period law requires us to keep them.
- **Support and sales correspondence, call recordings, marketing records and analytics** — for as long as they remain useful for the purpose described in Section 3, and no longer. The criteria we apply are whether the record is still needed to support the customer relationship, to evidence what was agreed, or to understand how the product is used.

You can ask us at any time what we hold about you, and ask us to delete it — see Section 13. We do not purge data from routine backup or archival systems on request; backups age out on their own cycle, and the information in them stays subject to the same protections for as long as it is there.

11. Security

We maintain a written information security program with administrative, physical and technical safeguards, including encryption of personal data in transit and at rest, role-based access control, logging and monitoring, and secure software development practices. All personal data is hosted in Microsoft Azure regions located in the United States. We do not operate our own data centers.

No system is completely secure. If a security incident affects your personal data, we will notify affected customers without undue delay and in any event within seventy-two (72) hours of becoming aware of it, and will notify individuals and regulators where the law requires.

12. Children

The Services are sold to businesses and are not directed at children. You must be at least 18, or the age of majority where you live, to hold an account. We do not knowingly collect personal information from anyone under 18; if we learn that we have, we delete it.

13. Your rights

Everyone. Whoever and wherever you are, you can ask us for a copy of the personal information we hold about you, ask us to correct it, ask us to delete it, and ask us to stop sending you marketing. We will do those things unless the law requires us to keep the information. We do not charge for this and we do not treat you differently for asking.

If the GDPR or UK GDPR applies to you, you also have the right to restrict processing, the right to data portability, the right to object to processing carried out on the basis of our legitimate interests, the right to withdraw consent at any time where consent is the basis, and the right not to be subject to a decision based solely on automated processing. Withdrawing consent does not affect the lawfulness of what we did before you withdrew it.

If you are in a US state with a comprehensive privacy law, you may have rights to confirm whether we process your personal data, to access, correct, delete and obtain a portable copy of it, and to opt out of sale, targeted advertising and certain profiling. We do not sell personal data, do not conduct targeted advertising, and do not profile in ways those laws cover. If we deny a request you may appeal by replying to our decision; we will respond to an appeal within the period your state's law allows and will tell you how to contact your Attorney General if you remain unsatisfied.

Making a request. Email privacy@welldatabase.com. We will verify your identity in proportion to the sensitivity of what is being asked for — usually by confirming control of the email address associated with the account. An authorized agent may act for you with written permission. We respond within forty-five (45) days, and will tell you if we need longer.

If your request concerns data we hold for a customer — data inside their WellDatabase account — we will refer you to that customer, who decides what happens to it, and will assist them in responding.

14. Complaints

If you are unhappy with how we have handled your personal information, tell us at privacy@welldatabase.com. We operate a complaints procedure: we will acknowledge your complaint within thirty (30) days, investigate it, and tell you the outcome.

You can also complain to a regulator. In the United Kingdom that is the Information Commissioner's Office. In the European Economic Area it is the supervisory authority in the country where you live, where you work, or where the problem happened. You do not have to come to us first, though it is usually faster.

15. Where information is processed

WellDatabase is a United States company and all of the personal information described in this policy is processed in the United States. Our subprocessors and their processing locations are listed at welldatabase.com/subprocessors.

Where we process personal data on a customer's behalf and a restricted transfer from the EEA, the United Kingdom or Switzerland occurs, that transfer is made under the European Commission Standard Contractual Clauses and, for the United Kingdom, the ICO's International Data Transfer Addendum, as set out in our Data Processing Agreement. We rely on those clauses rather than on the EU-US Data Privacy Framework. A copy of the safeguards is available from privacy@welldatabase.com.

Representatives in the EEA and the United Kingdom. WellDatabase does not currently offer the Services to individuals in the European Economic Area or the United Kingdom and has no establishment in either. Where we begin to do so, we will appoint representatives under Article 27 of the GDPR and Article 27 of the UK GDPR and identify them by name and contact details in this policy before that processing begins.

16. Changes to this policy

We may update this policy. When we do, we will change the version number and the effective date at the top, and keep the previous versions listed below. If a change materially and adversely affects your rights, we will give at least thirty (30) days' notice by email to account administrators, or by a prominent notice on the website, before it takes effect.

Version	Effective	What changed
2026.10	13 August 2026	Complete rewrite. Adds an effective

		date and version history; categories of information collected and categories of third parties; legal bases; disclosure of product analytics, session recording and call recording by name; retention criteria; Do Not Track and Global Privacy Control; the statement that we do not train AI models on personal information; the public-records section; a complaints procedure; and the international transfer position. Replaces the undated policy previously published at welldatabase.com/privacy-policy and app.welldatabase.com/privacy .
--	--	--

17. How to contact us

ctrlDev, LLC d/b/a WellDatabase

4 Waterway Square Place, Suite 477, The Woodlands, TX 77380, United States

Privacy and data protection: privacy@welldatabase.com

Legal notices: legal@welldatabase.com

Related documents: our Terms and Conditions at welldatabase.com/terms-and-conditions, our Data Processing Agreement at welldatabase.com/dpa, and our subprocessor list at welldatabase.com/subprocessors.